BEFORE THE
FEDERAL COMMUNICATIONS COMMISSION
WASHINGTON, D.C. 20554

In the Matter of	)	
	)	
Advanced Methods to Target and Eliminate	)	CG Docket No. 17-59
Unlawful Robocalls	)	
	)	
Call Authentication Trust Anchor	)	WC Docket No. 17-97

Comments of Noble Systems Corporation

Filed May 28, 2017

Karl Koster
Chief Intellectual and Regulatory Counsel
Noble Systems Corporation
1200 Ashwood Parkway
Atlanta, GA 30338

Noble Systems, a provider of contact center software and cloud-based service solutions, submits these comments in regard to the Commission's DECLARATORY RULING AND THIRD FURTHER NOTICE OF PROPOSED RULEMAKING[1], scheduled to be considered at its upcoming monthly meeting on June 6, 2019.[2] That document includes two portions, the first portion ("Declaratory Ruling") would allow carriers to block "robocalls" to their customers, by default, after determining such calls are unwanted and/or illegal. The carriers are presumed to employ analytics-based algorithms for determining whether such calls are robocalls. The second portion ("Third Further Notice of Proposed Rulemaking") includes a safe harbor for carriers blocking calls by targeting potentially spoofed calls identified using the "Shaken/Stir" standards.

The Declaratory Ruling portion: 1) allows voice service providers to block calls appearing to be illegal by use of analytics algorithms, 2) allows voice service providers to "whitelist" numbers in a consumer's contact list, and 3) reminds voice service providers that protecting emergency communications is paramount.[3] The exact scope of "emergency communications" is not defined, but it includes calls from public safety entities, including PSAPs, emergency operation centers, or law enforcement agencies.[4]

Presumably, this may even include emergency communications from schools. Would an automatic notification to a parent from their child's school regarding a cancelled after-school event be considered an emergency communication? What about an automatic notification that the child is not attending school today, and may be truant or missing? What about an automatic notification of a school emergency, such as a school shooting? All these calls may originate from the same originating telephone number. How can these be distinguished and properly categorized? Or, consider a power-outage notification call that informs affected residents of the expected power restoral time. Some may not consider this by itself to be an emergency call, but more of an informational call. But, if you are the caregiver for an elderly parent who is dependent on a portable oxygen generator, knowing how long the oxygen generator will be out-of-service makes this an emergency communication.

[1] FCC-CIRC1906-01, CG Docket No. 17-59, WC Docket No. 17-97.
[2] https://www.fcc.gov/news-events/events/2019/06/june-2019-open-commission-meeting.
[3] FCC-CIRC1906-01, par. 25.
[4] Id., par. 35.

The Declaratory Order creates an obvious, fundamental public safety issue. It does not define which types of calls and associated telephone numbers are "emergency communications." Second, it presumes that carriers will create a whitelist of such numbers that are not to be blocked. While a comprehensive list of such emergency numbers is unclear, specific numbers for local public safety, school, and police are easily identifiable to anyone with an Internet connection.

Thus, these emergency numbers are easily discoverable by scammers. Once scammers start to spoof emergency and public safety numbers, our public safety is at risk. If such calls cannot be blocked, then scam calls masquerading as public safety numbers will dilute the effectiveness of 'real emergency' calls. If such calls are blocked, then the Declaratory Order will be violated. Prior to deployment of Shaken/Stir technology, it is fundamentally unclear how carriers would comply in this circumstance.

By passing this Declaratory Order, the Commission creates a public safety risk. It is unclear whether the Commissioners voting on this have considered this risk and have a solution. One senior FCC staff member was asked a year ago: What will the FCC do if scammers start to spoof numbers from the FCC? An adequate answer could not be provided at that time. Now, it is appropriate to ask the Commissioners who are voting on this item: What will the FCC do when scammers start spoofing public safety numbers? Is the plan to address that problem when it happens? This Declaratory Order appears to be hastily drafted and was only recently made publicly available. This Declaratory Order may very well cause more harm than good.

The Commission presumes that uncertainty by the carriers has been an impediment to deployment of call blocking.[5] The Commission should ask whether this Declaratory Order clarifies uncertainty by the carriers as to exactly which communications comprise "emergency communications." The draft Declaratory Order does not address this uncertainty, but makes it clear that no adverse impacts to emergency communications are to occur.[6] Perhaps the real impediment to the deployment of call blocking by carriers has been the uncertainty how to address this problem?

[5] FCC-CIRC1906-01, par. 24 and 25.
[6] Id., par. 35.

An alternative path for proceeding would be for the Commission to excise the Declaratory Order portion and recast it as a separate Notice of Proposed Rulemaking. This would allow the Commission to solicit more comments on the impact, and understand why an implicitly defined whitelist for analytics-based call blocking is not a solution to the robocall problem. Fortunately, there is a solution to this problem, namely Shaken/Stir, and there are a host of relevant questions of how call blocking should be defined when both analytics-based blocking and Shaken/Stir-based blocking mechanisms are applied.

The Declaratory Order also fails to require carriers to deploy any type of blocking notification mechanism for analytics-based blocking. The importance of caller notification for Shaken/Stir-based call blocking is recognized by the Commission, as evidenced by the issues discussed in the Third Further Notice of Proposed Rulemaking portion. But, such discussion is noticeably absent for carrier-based analytics-based blocking in the Declaratory Order. Carriers blocking calls using analytics-based blocking could, at least, route the call to an intercept where an announcement informs the caller that the call is blocked. Such an announcement could inform the caller of a telephone number or website URL where they can seek mitigation of the blocking. Such an announcement would avoid use of "fake busy" treatment, which some carriers may be tempted to use. This, and other mitigation aspects related to analytics-based call blocking, were discussed with various industry stakeholders, including the FCC staff, in a series of meetings entitled "Communications Protection Coalition" ("CPC") that was sponsored by the Professional Association of Customer Engagement ("PACE"). A copy of the CPC's working document is included with these comments.

It is recognized that illegal and unwanted calls are highly problematic. The record shows nearly universal support for deployment of Shaken/Stir technology, but the same cannot be said for analytics-based call blocking. The Commission should maintain its focus on advancing Shaken/Stir technology and reconsider approving the Declaratory Order. The Declaratory Order portion should be excised and reconsidered as a Notice of Proposed Rulemaking.

Respectfully submitted on May 28, 2019,

/Karl Koster/
Karl Koster,
Chief IP and Regulatory Counsel
Noble Systems Corporation
1200 Ashwood Parkway
Atlanta, GA 30338
(404) 851-1331 (x1397)

Communication Protection Coalition ("CPC")

Report on

Best Practices for Mitigating Adverse Impacts of Robocall Processing on Legal Communications

Coalition Leader: Rebekah Johnson, Numeracle
rebekah@numeracle.com

PACE Task Force Leader: Karl Koster, Member of the Board of Directors,
PACEAnd Document Editor Noble Systems Corporation
kkoster@noblesystems.com

Contents

I. Introduction – Purpose

The purpose of this document is to summarize various best practices related to analytics-based call processing of robocall voice calls by service providers, referred to herein as "robocall call processing" ("RCP"). The Federal Communications Commission ("FCC") in its July 2015 Order (FCC 15-72) authorized service providers to block calls from being offered to their subscribers[1] in an attempt to mitigate the impact of illegal and unwanted "robocalls." In addition, although not addressed in that Order, service providers may "label" calls offered to their subscribers as a "robocall." While the exact scope of the term "robocall" is debated in the industry, for purposes herein, it is presumed to be a call which automatically plays a pre-recorded announcement to the called party upon the calling being answered. This is essentially the same definition of a "robocall" as used by the Federal Trade Commission ("FTC").[2] Other definitions are less structured, and refer to any call made by an automated device. Frequently, but not necessarily, such calls are unwanted and/or illegal. The FCC has used various definitions for "robocall", including a broader definition that includes any call initiated by an "autodialer." However, the scope of that term has been significantly debated in the courts. Regardless of the exact scope of the term "robocall", it should be evident, however, that the RCP principles and procedures herein have application to other types of calls (i.e., non-robocalls). Finally, while texts are frequently considered within the scope a "robocall", this document is focused on voice calls only.

The FCC has implicitly encouraged mitigation of certain aspects of robocall call processing in its July 2015 Order. The FCC stated that:

> In order to aid customers in making such informed choices, **we encourage technologies** designed for blocking incoming calls that are part of mass unsolicited calling events **to provide features that will allow customers to ensure that calls that are solicited**, such as municipal and school alerts, **are not blocked**, and that **will allow customers to check what calls have been blocked and easily report and correct blocking errors**. (FCC 15-72, July 2015, par. 161, emphasis added.)

[1] The FCC sometimes refers to "subscribers" as "customers." Throughout this document, the terms "subscriber", "called party", and "consumer" all refer to the same party.

[2] "If you answer the phone and hear a recorded message instead of a live person, it's a robocall." Comments of Kati Daffan, FTC. https://www.consumer.ftc.gov/media/video-0028-what-do-if-you-get-robocall

This document reflects the output of a cross-industry coordination effort, through a series of meetings hosted by PACE, to ensure that mechanisms are identified that "allow customers to check what calls have been blocked and easily report and correct blocking errors." In addition, mechanisms are also proposed to enable call originators to know which calls have been blocked, determine the blocking status of a number, and to request correction of blocking errors. The document also addresses related issues for call labeling. The goal is to ensure that legal and wanted communications are not unduly adversely impacted by robocall call processing, and this goal is achieved, in part, by providing a mechanism to mitigate errors when they occur.[3] This document includes methods and suggestions to minimize adverse impacts to both call originators and called parties, with respect to legitimate and wanted communications that encounter robocall call processing by a service provider. Because the methods and suggestions herein are advisory in nature, they should be viewed as a best practice. This document does not reflect any mandates nor commitments by the participants to implement any of the best practices described herein.

A. How This Document Was Developed

This document was the result of a coalition of various stakeholders involved with service-provider robocall call processing. An initial meeting occurred in Washington D.C., on September 20, 2017, involving various regulatory, carrier, call originators, consumer groups, companies, and industry associations. Subsequent meetings occurred on January 25, 2018; April 4, 2018; and September 26, 2018. A list of participating organizations is included in an Appendix to this report.

II. Basic Concepts

A. Glossary

1. **Robocall Call Processing** ("**RCP**") – at a high level, this refers to various methods for processing a call based on the premise it may be a potentially illegal or unwanted call of some form. In practice, RCP will be generally applied to legal and wanted calls as well. Thus, the distinction of illegal or unwanted is somewhat moot, since it cannot

[3] Hence, the task force name "Coalition to Protect Communications" ("CPC").

always be readily determined whether a call is wanted or illegal without additional facts. The application of RCP to a call does not necessarily always mean that the call will be blocked or labelled; the outcome may be to offer the call nonetheless with or without a label.

2. **Robocall** - this term has various meanings; some interpret this term to mean a call originating from an autodialer, an illegal telemarketing call, and/or a call in which a pre-recorded announcement is played. As used herein, it broadly refers to a voice call that automatically plays a pre-recorded announcement to the called party upon being answered. This does not preclude assigning a broader definition to the term, which some regulatory agencies have done.

3. **Call Labeling** - a form of RCP in which the call is offered to the called party, but with an associated display of a text-based label or icon of some form, which characterizes the call in some manner. For calls to a wireless number, a mobile application on a smartphone may be used in presenting the label to the called party. For calls to wireline number, the label may be indicated using techniques used to convey a calling name on a suitable caller-ID display device. A variety of labels could be indicated, such as e.g., “spam”, “scam likely”, “telemarketing”, “nuisance”, etc.[4]

4. **Call Blocking -** a form of RCP in which the call is not offered by the carrier to the called party, but is blocked. Some mobile applications can mimic call blocking by not alerting the user of an incoming call, but technically the call has been offered by the carrier to the user.

5. **Per-Call Blocking Indication** – an indication of some form informing the call originator that the current call has been blocked. This is in distinction to providing some other form of treatment, such as providing a busy signal, which does not explicitly inform the call originator that the call was blocked.

[4] Call labeling services are distinct from caller-ID services, which include calling name and calling number information. Caller-ID services have been provided to wireless and wireline subscribers for many years.

6. **Analytics-Based Carrier Call Blocking/Labeling** – this refers to processing done by the terminating service provider (i.e., carrier) acting on a call where the processing involves the application of analytics-based algorithms. Thus, a terminating carrier may block or label a call, including one that uses a facially valid, assigned, allocated number by using various analytics algorithms. Compare this to "non-analytics based carrier call blocking" defined below.

7. **Non-analytics-based Carrier Call Blocking** – this refers to call blocking actions, which may be performed by an originating, transit, or terminating carrier that examines the calling party number and determines it is an invalid, unassigned, unallocated, or unauthorized (i.e., do-not-originate) number and blocks the call on that basis. This type of processing for call blocking is distinct from call labeling, which is based on analytics.

8. **Mobile Application based Call Blocking/Labeling** – this refers to a mobile application operating independently of a carrier, which assigns a label to a call or suppresses user altering of an incoming call. The call is offered to the user's smart phone, but the mobile app may redirect or otherwise reject the call, but the call is not blocked or labeled by the carrier.

9. **Subscriber's Service Profile (for blocking/labeling)** – information specific to a subscriber as to how calls from a specific calling party number should be processed by a service provider.

10. **Service Provider's, Analytics', or Carrier's (blocking/labeling) Default Profile** – information maintained by a service provider/analytics provider/carrier as to the default treatment of how a calling party number should be processed for a subscriber. Information gleaned from various sources may cause calls using a particular calling party number to be blocked or labeled in a certain manner for all of the service provider's customers. However, a subscriber may indicate different treatment, i.e., overriding such treatment, by the information contained in the Subscriber's Service Profile.

B. Basic RCP Operation

For purposes herein, a "subscriber" is the called party who has their incoming calls subjected to robocall call processing, which typically occurs by the carrier or their analytics service provider just prior to offering that call to the subscriber. Specifically, the Calling Party Number ("CPN") and other properties associated with the call are analyzed in some manner to ascertain whether the call will be offered (if call blocking is provided) or to ascertain a label that may be associated with the call (if call labeling is provided).

In either analytics-based carrier call blocking or call labeling, the called party's service provider may analyze the aspects of the present call, use information collected from: other calls using that same calling party number, the subscriber's service profile, and other proprietary information in order to determine how to process the call.[5] Analysis is typically performed based on the CPN indicated in the call, taking into account other properties of the call event. If the called party is provided with a call labeling service, the service provider may query a database of some form and/or utilize proprietary algorithms to ascertain the appropriate label to be associated with the call. The label is usually a text-based word or phrase characterizing the call in some manner. Examples include, by way of illustration, "spam", "telemarketing", "nuisance" etc. There is no standard set of labels adopted by the industry. The call is offered in a manner such that the called party's phone device displays the label concurrently with alerting the subscriber of the incoming call. Thus, for example, a call to a mobile smartphone may display the label while alerting the user of the call. This typically requires a mobile application to be loaded in the smartphone. In some cases, the subscriber downloads the mobile application, in other cases, the wireless carrier may pre-load the mobile application on the phone when providing the smartphone to the subscriber.

On the other hand, a call to a wireline number may rely on a caller-id device that is capable of displaying, e.g., a calling name, but which instead is used to display the label. In this case, the

[5] There are other architectures in which the mobile app queries a database.

call may delivered to the called party with the associated label being displayed on the caller-id device. Other possibilities are possible, including using a computer or television to indicate the label in VoIP applications.

It should be noted that a user may download a mobile application for use on a smart phone that may interact with a third-party database, the operation of which may be independent of the user's carrier. While such operation is similar in outcome compared to a network provided RCP service, the operation of such is often outside the scope of this document, as the carrier may have no direction or control over the service provided by the third-party mobile app provider. Although the mitigation techniques described here are directed to carrier-based service providers, such third-party mobile application providers may benefit from offering similar mitigation techniques described herein.

If the called party subscribes to call blocking from their service provider, the service provider will use an algorithm to ascertain whether the call is to be offered or blocked. If the call is to be offered, then the call proceeds as normal (the call may still be subject to call labeling). If the call is to be blocked, then the service provider should provide some indication of such to the call originator. While many advocate for an explicit per-call blocking indication of some form indicating the call has been rejected, others advocate for providing treatment that is not definitive of indicating the call was blocked, such as busy treatment.

The indication that a call is blocked call can occur in different ways and the approach depends on part on the technology used by the call originator to interface with their service provider. However, it is recommended that the rejection indication accurately convey the processing encountered by the call, as opposed to indicating call treatment that is a misleading or unclear. Several possible approaches to indicate that the call was blocked due to RCP include providing distinct in-band audio and/or out-of-band messages signifying the call was blocked to the call originator. There are several variations of in-band audio information that can be provided to indicate a call is blocked, including:

a) ***Special Information Tone ("SIT tone").*** This is a sequence of three tones – a 'tri-tone' – that may convey a busy condition, disconnected number, or some other condition. It may be accompanied by an announcement.

b) ***Audio tone****.* An audio tone indicating "busy" may be provided (i.e., a busy tone). This is a familiar tone, designed to be recognized by a human being, reflecting that the called party's line is busy. However, using this tone creates uncertainty to the call originator as to whether the line is actually busy or whether the call was blocked.

c) ***Intercept Announcement****.* This is a recorded announcement or synthesized speech designed to inform a human listener of a specific condition. Networks may provide an intercept announcement in other cases, such as when the called number is disconnected or reassigned. A dedicated intercept announcement could be defined informing the call originator that the call was blocked.

The out-of-band messages that could convey the call has been blocked include:

a) ***ISDN cause code information****.* If the call originator uses an ISDN interface, such as a Primary Rate Interface, a message rejecting the call will be received at the call originator with a cause code. The value selected depends on the value determined by the service provider performing the RCP.

b) ***HTTP error code information.*** If the call originator uses a VoIP interface with, e.g., SIP signaling, an HTTP status code may be received. One example frequently encountered when surfing the web is the ubiquitous "Error Code 404 – Not Found." A corresponding code can be defined for blocking SIP calls.

For carrier-based call labeling, the call originator is not provided with any indication that the call has undergone any RCP related to call labeling. In practice, the called party may opt to forego answering the call based on the label value indicated on the call. If so, conventional call processing will take place in response to the called party not answering the call. For example, if the called party has a voice mail service, the call may be forwarded to the voice mail server if the called party does not answer the call. If the called party has an answering machine, it may answer the call if the called party does not answer.

III. Called Party Election of RCP

The called party is presumed to have elected to receive RCP, regardless whether the processing involves call labeling or call blocking. With respect to call blocking (not call labeling),

the FCC has indicated in its July 2015 Order that the customer must opt-in or subscribe to the service.[6] Further, the FCC has indicated that consumers can "drop such services" if they find their accuracy unacceptable.[7]

The FCC has not mandated whether consumers must opt-in (and correspondingly, opt-out) for call labeling services. However, in light of comments by the FCC in regard to call blocking, namely "Consumer choice has been important to the Commission in previous decisions, and continues to be important"[8], it appears reasonable to infer that consumers should have the choice to opt-in to receive call labeling. Many wireless carriers provide caller ID services, such as calling number delivery, and by default and they may choose to augment their services to include calling name, or call labeling. If so, it is presumed that consumers will be provided mechanisms to opt-out to call blocking and potentially to call labeling. This could be implemented as simply providing an "off" or "disable" function for the mobile application to disable the display of call labels.

IV. Mitigation of Robocall Call Processing

A. Introduction

RCP mitigation involves two perspectives: the call originator (a.k.a. calling party or caller) and the called party. The called party is presumed to be a subscriber of the RCP service from their service provider (hence, the term "subscriber" may be used). The call originator is not necessarily a subscriber of the same service provider serving the called party.

B. Call Originator's Perspective

The call originator's concerns with respect to mitigating a call that is subject to robocall call processing involves:

[6] See, e.g., "Indeed, there appears to be no legal dispute in the record that the Communications Act or Commission rules do not limit consumers' right to block calls, as long as the consumer makes the choice to do so." (FCC 15-72, par. 156, see also par. 154, regarding "offering consumers the choice, through an informed opt-in process…")
[7] See, e.g., *Id.*, par. 160.
[8] See, *Id.,* footnote 504.

- **Awareness**. The call originator needs to know that a call they originated was blocked (for call blocking) and preferably would know how it was labeled (for call labeling). Without knowing if a call was blocked, the call originator has no indication that further mitigation procedures may be required to correct erroneous blocking. While the call originator is preferably informed in real time when a call is blocked, the call originator has no mechanism to be informed on a per-call basis what label was used.
- **Identify the Called Party's Service Provider**. The call originator needs to identify the service provider associated with the called party performing the RCP in order to request mitigation of the impact of erroneous processing, such as erroneous blocking or inaccurate labeling. Typically, the call originator has to identify a different service providers for different called parties.
- **Identify Appropriate Contact Channels.** The call originator needs to be aware of the channel(s) and addresses used to contact the called party's service provider for purposes of attempting the mitigation. For example, various service providers be contacted by email, voice calls, accessing a web page, etc. to receive a mitigation request.
- **Mitigation.** Once the appropriate service provider is identified, along with the appropriate channel to submit a mitigation request, the call originator needs to interact with the service provider for purposes of mitigation. The details of how this occurs is service provider specific, but examples are provided herein.

1. Awareness – Knowing When a Call Encounters Call Blocking (Per-Call Blocking Indications)

A call that encounters analytics-based carrier call blocking will be rejected in some form and the carrier will not offer the call to the called party's interface. It is preferable that an accurate signaling indication be provided to the call originator. The indication should accurately reflect the call has been blocked, as opposed to, e.g., providing a response indicating the called

party is in an alleged "busy" condition.[9] Consequently, it is preferable to inform the call originator the call was blocked in an unambiguous manner. It is expected that call originators will respond to the signaling indication by ceasing originating subsequent calls to that called party. Service providers may not necessarily notify a subscriber (i.e., the called party) when a call has been blocked in real-time, but they should allow the called party to review, in some manner, which calls have blocked.

A service provider that labels a presently does not indicate to the call originator that the call was labeled. Thus, the call originator has no direct mechanism of knowing whether or what type of a call label was associated with the call. However, it is a best practice to offer callers a mechanism to query the service provider (or their associated analytics provider) to inquire (at the time of the query) whether a particular CPN is associated with a label and provide information reflecting what that label value. There is no guarantee that the label value may not have changed since the response was sent or just prior to receiving the query.

a) Call Blocking Treatment

Call blocking treatment defines the treatment provided to a call originator when the terminating service provider blocks the call based on analytics-based carrier blocking processing. The call originator should be provided a signaling indication of some type that indicates that the call was blocked due to RCP, as opposed to information reflective of some other condition (such as a conventional user busy condition or disconnected number).

(1) In-Band Audio Provided

Preferably, in-band information comprising a recorded announcement (called an intercept announcement) would be played to the calling party when the call is blocked. This intercept would indicate to the caller that the service provider has blocked the call and inform the caller that if they believe this is in error, they should contact the service provider. Contact information may be provided in the intercept.

[9] Because the Call Originator cannot differentiate between an erroneously reported busy condition due to call blocking and a "true" busy condition based on the called party's interface, the Call Originator may attempt to originate the call again to the called party at a later time. This subsequent call can be expected to receive the same treatment, which may again result in another call origination attempt.

The provision of an intercept is commonly used today to indicate disconnected numbers to callers. Intercepts can be to the caller regardless of the various technologies used to establish the call (such as conventional public switched telephone networks, ISDN, SS7, wireless, VoIP, etc.).

(2) Out-of-Band Cause Codes Provided

Cause codes are signaling elements conveyed back to the originating switch indicating what treatment a call is currently receiving. Cause codes are defined in specific telephone signaling networks to indicate when a call cannot be completed because of various conditions, such as busy, network congestion, number out of service, etc. It is recommended that a cause code be used that unambiguously indicates the call has been blocked. In SIP technology, these are referred to as "error codes." These codes are defined for each telephony signaling standard and must interwork amongst each other.

It is not as critical for carriers to provide a per-call blocking indication to the call originator in cases of non-analytics-based call blocking. Typically, non-analytics-based call blocking functions to block facially illegal calls. Thus, a transit carrier blocking calls based on detecting an invalid, unassigned, or unallocated number may not return a per-call blocking indication, because it is presumed that such calls are facially illegal. There is less industry motivation to providing accurate blocking information to call originators who appear to be originating illegal calls.

b) Call Labeling Treatment

An originated call that encounters call labeling will be labeled by the terminating service provider in some form when the call is offered to the called party. No particular signaling is conveyed to the call originator indicating that call labeling has occurred. Thus, the call originator may find out via anecdotal evidence (or not at all) that the call was delivered with some form of RCP labeling treatment. However, the service provider should provide a mechanism allowing the call originator to query and ascertain whether a label is associated with a CPN, and what is the corresponding label value.

The mechanism could be an application programming interface ("API") and/or web page where a number can be provided by a user and a corresponding response received. It may be necessary to limit who can initiate such queries. Security reasons may dictate identification information is required to limit access to legitimate call originators who have registered the

particular number. A separate, but similar mechanism may be defined allowing the called parties to check with their service provider for this information for their past received calls.

2. Identification of RCP Service Provider

The call originator requires a mechanism to identify the service provider of the called party based on the called telephone number. This can be accomplished in various ways. Various Internet-based tools are readily available that will accept a telephone number and return the name of the serving carrier. These tools are designed to receive a single, manually entered number, and return the designated carrier. If a large quantity of numbers are to be processed to identify a plurality of service providers, then some other mechanisms may be necessary. It is also possible that third-party entities may provide a service to call originators to facilitate registration, identification of service providers, and handling of mitigation requests.

3. Identifying Mitigation Contact Channels

The service provider should make available a contact channel and address, such as in the form of a web site, which can be used by the call originator to initiate the mitigation request. With respect to call labeling, the mitigation process may involve the call originator requesting an alternative label to be associated with the calling party number in lieu of the one indicated. With respect to call blocking, the mitigation process basically involves requesting a particular number to be unblocked. However, it shall be at the discretion of the service provider as to whether a request from a call originator shall be acted upon.

4. Processing the Mitigation Request

The process for handling a mitigation request is defined by the service provider. The mitigation of a request involves acting on a request from the Call Originator to: 1) inquire about the status associated with an identified CPN(s), or 2) modify the RCP procedures associated with a CPN. Typically, the request is to unblock calls, i.e., allow calls from a specified CPN to be offered that were previously blocked. Or, the request is to review or modify the label associated with the CPN when the call is offered to the subscriber. The definition of these procedures (whether and on what basis the service provider acts on these requests) are outside the scope of this document.

a) Called Party Registration

It is expected that service providers will require call originators to register prior to acting upon a mitigation request. Registration requires the call originator to identify themselves in some manner, so that the service provider can "vet" the call originator. This is based on the assumption that legitimate call originators are willing to register, whereas illegitimate call originators will not. Registration is intended to preclude "bad actors" or "scammers" from requesting mitigation of their calls.

Registration is expected to involve a call originator providing information comprising:

- Contact Name of Individual
- Title
- Company and Organization Name, address
- Contact information (email and phone number)
- List of number blocks used by organization for outbound calls.

The information requested by a service provider for registration may vary. Further, additional information from what is shown may be requested. The purpose is to allow the service provider to ensure the call originator is a legitimate call originator, however they make that determination. It may be necessary for the call originator to identify the list of telephone numbers it uses for call origination. Further evidence or declaration may be requested evidencing that the call originator is authorized to use such numbers. Situations should be accommodated where call originators are not assigned numbers by a carrier, but are authorized by the entity that is assigned those numbers to originator calls on that entities behalf (i.e., the call originators are authorized to spoof the number).

One example of registration information request is provided below.[10] The information may comprise:

1) Call Originator Information

The following contact information that may be collected by a third-party vetting entity about the call originator.

[10] Courtesy of First Orion, see www.calltransparency.com. No endorsement is implied by incorporation herein.

- Contact Name – name of the person to address issues requiring human intervention
- Contact Phone Number – to reach the person designated above.
- Contact Email Address – used to potentially send alerts/notifications regarding abnormal telephone number usage
- Company Name – entity responsible for originating calls
- Company Address
- Website
- Estimated Call Volume (e.g., calls/Month)
- Service Provider Client's Name (if call originator is a service provider originating calls for others)
- Comments

2) Calling Number Information

The following telephone number information may be collected at registration to provide information about each registered calling number.

- Calling Telephone Number
- Industry Type
  - Personal
  - Education
  - Emergency Service
  - Finance
  - Health
  - Nonprofit/Charities
  - Pharmacy
  - Political
  - Prison/Jail
  - Publishing
  - Technology
  - Retail
  - Utilities
  - Other Industry
- Call Purpose
  - Personal – calls made for personal reasons
  - Telesales/Solicitations – calls made to induce the purchase of a product or service or solicit a contribution or support either financial or otherwise. It includes solicitation for political or charitable purposes
  - Survey – calls made for the purpose of conducting a survey or market research
  - Loan Servicing – calls made by the loan originator to service the account including delinquent reminders
  - Account Services – calls made for the purpose of collecting a delinquent debt or other financial account matters

- Preferred CallerID Name (optional)

Registration occurs only once for a call originator for a given service provider, and the mechanism to accomplish this is not necessarily automated. Thus, the call originator may have to register with multiple service providers using different, manual processes. The process of registration and the associated vetting of the numbers indicated should be accomplished within a few business days or sooner (preferably). Upon completion, the service provider will provide the call originator with credentials, such as a User ID and Password for access to a website in order to: update information, request registration of additional telephone numbers, or submit a mitigation request (either inquiring of a status or requesting the change of status of a number(s)).

b) Status Request

A call originator can make a request to a service provider of the blocking/labeling status associated with a calling party number ("CPN") or set of CPNs. Different mechanisms may be offered by a service provider depending on whether the request is for a single number or a list of numbers. However, in both cases, the response provided indicates the status of that number at the time the response was processed.

The status of a number, whether it be its associated label or blocking status, may change at any time. Thus, it is quite possible that a number may have one status (such as being blocked), which prompts a call originator to inquire of the status, but by the time the inquiry is handled, the analytics algorithm may have altered the status (to be unblocked). Thus, the resultant status is only valid at the time the request was processed, and it should be recognized that the status is not a static value.

A response to a request for the status of single number should be returned in real-time, whereas as a request for a list of numbers comprising e.g., 100 or less, should be normally returned within a few minutes. A list greater than 100 should be normally returned within 1 business day.

c) Request to Change Status of a Number

A call originator can submit a request to alter the label or blocking status of a number, but there is no assurance that any such request will result in a change. A response from the service provider may provide a "reason code" if the status of a number was not changed as requested. Some reasons include the following:

1. Requested status of the indicated CPN is already in that state. No change has been made.
2. Called Party has requested any received calls with that CPN should be blocked or labeled in a specific manner.
3. Called Party has requested any received calls of the type associated with the indicated CPN to be blocked, and calls from the CPN were accurately determined to be of that type.

The reason code should distinguish between a status allocated to a number by a called party explicitly (i.e., as in the subscriber's profile) versus a status generally determined by the service provider based on analytics. Specifically, if the called party has indicated calls from that CPN should be blocked or labeled in a certain manner, a call originator typically cannot override such indications based on the caller's request. A call originator in such cases may have to contact the called party via other means and request that the called party submit a change request to their service provider. Specifically, the call originator may have to contact the called party and ask that they 'unblock' their calls if the called party wishes to receive such calls.

In other situations involving call labeling, the analytics algorithm may have determined the call is properly labeled. The call originator may have to escalate the issue with the service provider to alter how the CPN is labeled. Alternatively, the call originator can request the service provider assign a specific label for that CPN. For example, a call originator may request their CPN be labeled as e.g., "informative" instead of "telemarketing", but the analytics provider may assert that the proper label, is in fact, "telemarketing."

A response to a request to alter the label status from a call originator should be returned within one business day. If the call originator disagrees with a refusal to alter the status, the call originator may escalate the issue with the service provider via other channels, or with regulatory authorities if appropriate.

C. Called Party's Perspective

The called party presumably has opted-in to receive the RCP blocking service, in accordance with the FCC's Order. With respect to call blocking, the called party may want to ascertain or review which calls were blocked, and request that certain CPNs be "unblocked" when the call is directed to them. However, providing an RCP labeling service does not necessarily require a subscriber's opt-in and hence there may not be an "opt-out" mechanism provided. With respect to call labeling, when the called party receives the call, they are presumably aware of the associated labeling at the time of presentation. However, if the called party finds that the label is inaccurate, then the called party may choose to inform their service provider of the error.

1. Review of Calls Subject to RPC

A called party should be able to review which calls were not offered to them because of call blocking. There is no corresponding need to inform the called party which calls were labeled, but a service provider may provide such information to the called party for other purposes (e.g., allowing a customer to review past incoming calls along with their labels). Review of blocked calls may be provided by the service provider by offering a web site to provide the information of blocked calls to the called party. Call detail information can convey the times, dates, originating CPN of the call, and optionally, the reason why the call was blocked.

2. Identification of Channel Used to Submit Mitigation Requests

The called party should be made aware of the channel and address used for submitting requests for mitigation. This could be a customer service telephone number and/or a web site published on the service provider's website or billing statement.

3. Mitigation of Calls Incorrectly Blocked or Calls Mis-Labeled

Once the called party is aware of a problem with how their calls are being processed, e.g., the called party encountered wanted calls that are being blocked, or calls that are offered are improperly labeled, the called party should have a means to mitigate the undesired RCP with their service provider. This occurs by the called party interacting with a customer service agent and/or the above mentioned self-service web site.

For call blocking, the service provider should provide their subscribers (i.e., the called party) with a mechanism to indicate that a particular CPN should not be blocked (if presently blocked) or should be blocked (if not presently blocked). In one method, the called party can review a listing from their service provider of blocked calls, select a call and its corresponding calling party number, and request that call to be blocked or unblocked as appropriate. The blocking status of each CPN is then unique to that called party. That is, a different called party may elect to have that same number processed different from another called party.

For call labeling, the called party may be provided with a mechanism to indicate to their service provider that the call should be labeled using some other label, or none at all. This may involve maintaining a subscriber profile the stores the called party's labeling preferences. If provided, then the service provider would have to maintain a customer-specific determination of the label for each calling party number.

V. Use of a Third-party to Facilitate Registration or Vetting

a) Calling Party Registration

"Calling Party Registration" (or merely "Registration") refers to a voluntary process where call originators provide information related to their call originations to a service provider (i.e., either a telecom carrier or its analytics provider) terminating its calls. The registration process may interact with a telecom carrier directly, or the telecom carrier may direct the call originator to interact with its corresponding analytics provider. The registration process will be frequently replicated by the call originator among a number of carriers/analytic providers, since the call

originator will likely be directing calls to various destinations served by a variety of terminating telecom carriers.

It is expected that some service providers will require call originators to register as a precondition prior to acting upon a call blocking or call labeling mitigation request. A concern of service providers is that scammers, upon learning their calls are being blocked or labeled as such, will initiate a mitigation request with the service provider so as to avoid having their calls being blocked or labeled. Thus, one of the functions the service provider is expected to perform before addressing a mitigation request is to ensure that the call originator is not a scammer, i.e., "vet" the call originator.

To facilitate the process, a call originator may enlist the aid of third-party service provider that will act as a proxy for the call originator and register the call originator with various carrier/analytic entities. This third-party service provider essentially can vet the call originator on behalf of the carrier/analytics provider and further coordinate registration among different service providers. There are expected to be various third-party vetting entities which will provide these vetting/registration services. These third-parties may be consultants, industry associations, law firms, telecom providers, etc.

The level of vetting may be extensive or perfunctory. If the latter, then the vetting entity is acting more as a registration entity to aid in registering the call originator's numbers with the various carriers/analytics entities. It remains to be seen how market forces will determine what constitutes an acceptable or minimum level of vetting.

The vetting process is intended to allow legitimate call originators successfully pass through the process, whereas illegitimate call originators will be presumably identified as scammers. In addition to relieving carriers/analytics providers from this responsibility, a third-party vetting provider facilitates the registration process for the call originator, as they can avoid having to navigate potentially different registration processes and identify all the possible service providers to register with. The relationship can be illustrated as shown in FIG. 1.

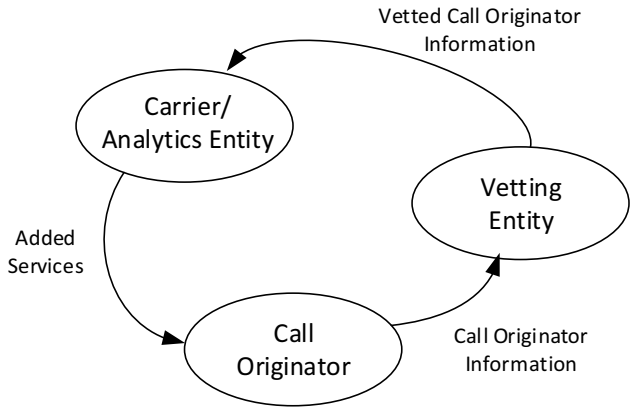

Fig. 1

The call originator provides various information to the vetting entity, which may validate the call originator's information. The vetting entity then interacts with each carrier/analytics provider according to their corresponding procedures to provide the call originator's information, which has been vetted. The carrier/analytics provider may use that information to provide added services to the call originator. For example, if the call originator's calling telephone numbers begin to exhibit usual calling patterns, which may be attributed to a third-party spoofing that number, the carrier/analytics provider may contact and inform the call originator of the anomaly. Thus, the call originator receives value added services that inform them of a spoofing campaign using their telephone number that has been detected by the carrier/analytics provider. In other instances, the vetting provider may receive such information from the carrier/analytics provider and in turn inform the call originator of potential concerns.

The information requested by a service provider or a vetting entity may vary, and likely will include further information that the minimum information described above. The purpose of information provided to the vetting entity is to ensure the call originator is legitimate and to ensure the carrier/analytics provider accurately processes calls using that calling party number. For example, the vetting entity may solicit information from a call originator relevant to establishing their legitimate status, such as their industry classification and registered corporate business name. The information collected may vary, as it could include, for example, licensing information if the call originator is a licensed debt collector, number of years in business, Better

Business Bureau ("BBB") status information, public/private status, etc. However, the carrier/analytics provider likely does not need to know all these aspects, but may benefit from a subset of information allowing it to determine whether the call origination patterns fit a certain call origination profile. For example, the carrier/ analytics provider upon being informed the call originator is a debt collector may associate certain call origination patterns derived from calls that are frequently associated with a debt collector.

The purpose of the contact information provided to the service provider is to facilitate investigation of potentially abnormal traffic patterns and to potentially notify the call originator if something is amiss. For example, it is anticipated that some service providers may provide notifications to a call originator if a spoofing campaign is detected using one of the registered numbers of the call originator.

In addition to identifying the list of numbers (or ranges) used in call origination, information about traffic characteristics may be requested by the vetting entity and/or provided to the carrier/analytics entity. The form of the information may vary, and its purpose is to determine traffic characteristics to accurately process the calls from that originating telephone number. For example, knowing that a call originator is a debt-collector will provide some information as to what type of traffic characteristics can be expected.

b) Added Services Provided to the Call Originator

Each service provider (i.e., carrier/analytics provider) may have separate procedures and information requirements for completing registration. Once a number is registered, there may be further value-added services provided by a carrier/analytics provider to a call originator. One benefit of registering to a call originator is that the carrier/analytics provider can associate an accurate label with calls using that number, as opposed to using a potential default label of "scam" or "spam." Even if the number has been registered, it is possible that the service provider's analytics algorithms may detect a large unexpected call volume originating from a calling number that is given a label of "spam" or blocked as such. If the service provider knows, for example, that a calling campaign has just started using the calling party number, then a call

label can be assigned that is more closely associated with the indicated purpose of the call, and may avoid allocating a "spam" label.

If the service provider knows information about traffic characteristics of that telephone number, then the service provider may allocate different threshold levels that trigger certain call treatment. For example, a service provider may have traffic threshold levels that are used to trigger assignment of a "spam" label or invoke call blocking. If the service provider is aware of expected traffic characteristics in advance, the service provider may be able adjust those default threshold levels and avoid inaccurately labeling or blocking the calls. Thus, a call originator informing a service provider of an anticipated large volume of calls may avoid otherwise adverse or incorrect treatment of those calls.

The service provider may also provide notifications or alerts to the call originator upon detecting an unusual or unexpected level of traffic associated with a telephone number. For example, a financial institution may find that one of its numbers is being spoofed as part of a scam. A service provider upon detecting a large number of calls from that number, or complaints identifying that telephone number, may elect to inform the call originator who registered the telephone number of the situation. This allows the call originator to cease originating legitimate calls using that telephone number, which will avoid the service provider from mislabeling legitimate calls as "scam" during the spoofing event. This will result in the actual "scam" calls that are spoofing the number to be accurately labeled. In response of such notification, the call originator may choose to retire that number, as least temporarily, from use in legitimate calling campaigns.

Registration typically occurs once for given number to a call originator, and the process of registering numbers should be confirmed by the service provider within a reasonable time period, such as within one to two business days, if not in real time. Once the call originator is vetted and registered, subsequent registrations of additional telephone numbers by the call originator may be required, and are expected to occur in faster, as the call originator has already been vetted.

c) Use of a Vetting Entity May Be Optional

Carriers/analytics providers may interact with call originators directly, or may direct them to a third-party vetting entity. No requirement is implied as to whether a carrier/analytics provider requires call originators to use a third-party vetting entity.

Upon completion of registration, the service provider will provide the call originator or vetting entity with a User ID and Password for future access their web site to update information for that call originator, request registration of additional telephone numbers, or submit a mitigation request (either inquiring of a status or requesting the change of status).

VI. Number Management to Mitigate RCP Impacts

"Number management" broadly refers to how a call originator can manage the use of the CPN so as to minimize the likelihood of the number being blocked or otherwise adversely impacted by RCP. This form of mitigation seeks to prevent undesirable RCP impacts by the way in which multiple calls originate using that CPN. This typically applies to call originators originating a large number of calls and suggests how a pool of CPNs can be effectively used. Many call originators will find collaborating with RCPs beneficial for optimizing their call origination performance. Such collaboration may occur via specific channels between the call originator and service providers, and is outside the scope of this document.

VII. Disclaimer-Conclusion

The procedures defined herein are generic guidelines only, and are not meant to be binding on any particular carrier or service provider. However, it is in the best interest of the service provider to minimize errors in blocking or labeling a telephone number, and hence to reduce the need for RCP mitigation by callers or called parties. Because errors are recognized as possible, correcting such errors in a timely manner will allow the benefits of call labeling/blocking to be maintained.

APPENDIX – Participating Organizations

ENTITY NAME	Sept. 20 2017	Jan. 25 2018	April 4 2018	August 3 2018
ACA International	x	x	x	x
ADT	x			
Alorica		x	x	x
Altisource	x		x	x
American Bankers Association	x		x	
ARDA (American Resort Development Assoc.)	x		x	
AT&T	x	x	x	x
ATIS			x	
Call For Action			x	x
CenturyLink				x
Comcast	x		x	
CFPB			x	x
Contact Center Compliance	x	x	x	
CSG	x			
Customer Count	x	x	x	x
Ericsson				x
Eckert Seamans			x	
Federal Communications Commission	x	x	x	
Federal Trade Commission	x	x	x	
First Orion	x	x	x	x
Highlights	x			
GAO				x
Hiya	x		x	
iconnectiv	x			
Insidearam.com			x	x
Kelley Drye	x	x	x	x

MacMurray Shuster	x		x	x
MRSBPO	x			
National Association of Federally Insured Credit Unions (NAFCU)	x		x	
Neustar		x	x	x
NobelBiz		x	x	
Noble Systems	x	x	x	x
NTCA	x			
Numeracle	x	x	x	x
Ontario Systems	x			
PACE	x	x	x	x
Quality Contact Solutions	x			
Rural Wireless Association			x	
SiriusXM	x		x	
Sitel	x			
SOCAP	x			
Start Point	x			
Sprint			x	x
The IA Institute	x	x		
TNS	x		x	
Triwest Communications	x			
USTelecom	x		x	x
Verizon	x	x	x	x
ZipDX			x	x